UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

SECURITYSCORECARD, INC., Plaintiff, -against- SAFE SECURITIES, INC. d/b/a SAFE SECURITY and MARY POLYAKOVA, Defendants.	Case No. 24-cv-04240 **FIRST AMENDED COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, SecurityScorecard, Inc. ("SSC" or the "Company"), by and through its undersigned counsel, for its Complaint against Defendants Safe Securities, Inc. *d/b/a* Safe Security ("SAFE") and Mary Polyakova ("Polyakova," together with SAFE, "Defendants"), alleges as follows:

NATURE OF THE ACTION

1. While brazenly touting a "revolutionary" approach to cybersecurity risk management, Defendant SAFE's only true "revolution" is its unconstrained reliance upon unlawful skullduggery and unfair competition to build its business. As detailed below, this has to date included: (1) hiring a senior SSC sales executive, who brought with her stolen SSC customer and prospect lists with approximately 9,300 proprietary entries — entries assembled at a cost to SSC in excess of $40 million; (2) impermissibly accessing SSC's customer platform through a proxy and downloading SSC's work product to enhance and improve SAFE's own competitive product offerings in clear violation of contractual and legal prohibitions on SAFE doing so; (3) impermissibly browsing the features and functionality of SSC's customer platform through a proxy

to surreptitiously quality check, and reshape, SAFE's own customer offerings, in clear violation of contractual and legal prohibitions on SAFE doing so; and (4) using deceptive employee interview pretexts to try to uncover SSC's confidential plans. And, this is merely what SSC has uncovered thus far, with limited discovery.

2. Even when caught in this web of deceptive wrongdoing, SAFE has simply adopted a "deny, deny, deny" posture, effectively doubling down on their unlawful conduct. That's precisely what necessitates the injunctive relief now sought here, to put an end to these unlawful practices and protect SSC's trade secrets and confidential and proprietary information from further exploitation by SAFE.

3. Plaintiff SSC, the global leader in the security ratings space, helps businesses and governments identify their cybersecurity vulnerabilities, and mitigate cybersecurity threats. SSC utilizes cutting-edge analytics to provide its customers a critical tool to prevent cyberattacks.

4. Since its inception, SSC has spent over $200 million assembling its full customer and prospect base. SSC offers those customers state-of-the-art cybersecurity risk analysis and a broad suite of cybersecurity consulting services.

5. Defendant SAFE, a relative newcomer to the security ratings space, is a direct SSC competitor. In an attempt to gain market share directly from SSC, in 2023, SAFE launched an aggressive marketing offensive that included making derogatory statements about SSC to the media and arranging bogus job interviews with SSC employees to learn about SSC's business.

6. SAFE currently devotes an entire page of its website to trying to distinguish its services from SSC's. *See* https://safe.security/safe-vs-securityscorecard/ ("Why Customers Choose Safe Over SecurityScorecard?").

7. SAFE upped the ante by impermissibly accessing SSC's platform for competitive purposes, through a proxy in India, in direct violation of SSC's end-user SaaS agreement (the "User Agreement"). That User Agreement, attached hereto as Exhibit A, clearly prohibited SAFE from accessing SSC's platform "to build a competitive product or service or use [the platform] in a way that competes with products or services offered by SSC." *Id*.

8. SAFE openly admits its impermissible use of SSC's customer platform for such competitive purposes, touting that its own webpage comparison of SSC and SAFE is based on its "review done May 2024." *See* https://safe.security/safe-vs-securityscorecard/.

9. SSC's platform maintains various materials and customer offerings including action plans, detailed reports, digital footprints, issues reports, questionnaire templates, and scorecards ("Platform Materials").

10. SAFE admits accessing the SSC platform through paid accounts registered under the name of a proxy in India, so that SAFE could surreptitiously access SSC's platform under a cloak of fakery and download and export SSC's Platform Materials to gain an unfair competitive advantage over SSC.

11. Equally reprehensible is SAFE's attempt to gather intelligence about SSC by conducting bogus interviews with SSC employees with no intent to hire them, in a sweeping covert campaign to learn SSC's business strategy.

12. But SAFE's latest, and by far most egregious unlawful maneuver, is the hire of Polyakova, whom we now know secretly misappropriated a treasure trove of SSC trade secrets and confidential and proprietary information shortly before her departure from SSC. This misappropriation includes highly-detailed confidential information about approximately 9,300 SSC customers and prospects.

13. The information stolen by Polyakova includes an excel spreadsheet providing detailed confidential and proprietary information about 9,262 SSC customers and prospects in its East region (the "Master East List"), a document Polyakova emailed to her personal GMail email account. This Master East List includes each customer's annual recurring SSC revenue, projected future annual recurring SSC revenue, contract end dates, SSC licenses purchased and consumed, "business alliance partners,"[1] activity on SSC's platform, SSC's individual contacts at the customer, and the customer's location (*i.e.*, state or geographical region).

14. Polyakova also stole two files containing detailed confidential information about over 200 CISO (Chief Information Security Officer)-level SSC prospects, and the individual contacts at each such prospect, information compiled by SSC as a way to track invites and RSVPs to two business development events (the "CISO Prospect Lists").

15. On May 21, 2024, SSC discovered that, on January 4, 2024, Polyakova sent the Master East List to her personal GMail email account and that, on March 27 and 28, 2024, Polyakova sent the CISO Prospect Lists to her personal GMail email account.

16. The forensic proof SSC has uncovered of this theft is irrefutable and establishes Polyakova's flagrant disregard of her SSC employment contract ("Employment Agreement"), SSC's U.S. Employee Handbook ("Employee Handbook") and SSC's Acceptable Use Policy ("Acceptable Use Policy"), attached hereto as Exhibits B, C, & D, respectively.

17. Polyakova stole the Master East List and CISO Prospect Lists, upon information and belief, so she could share that information with SAFE, and use that information for SAFE's benefit, as its newly-hired Vice President, Central Sales, and thereby facilitate SAFE's unlawful

[1] Business alliance partners are SSC's strategic partners that enable SSC to reach specific target markets or bundle SSC services with another company's offering. With this information SAFE could directly access SSC customers through alliance partners connected to those customers.

poaching of SSC's customers and prospects. Polyakova announced on May 30, 2024, on LinkedIn, that she had joined SAFE. *See* Ex. E. In that same online post, Polyakova states she is seeking to hire sales representatives in six of the states specifically covered in the Master East List. *See id*.

18. To preserve the status quo, and block SAFE and Polyakova from succeeding in their unlawful attack on SSC's core security ratings business, SSC now seeks injunctive relief:

(1) enjoining Polyakova, SAFE, and all persons acting in concert with or through them who receive actual notice of the injunction, from using or disclosing the Master East List, the CISO Prospect Lists, the Platform Materials or any other SSC trade secrets or confidential or proprietary information (collectively, "Confidential Information");

(2) enjoining Polyakova from further breaching the confidentiality obligations contained in her Employment Agreement with SSC;

(3) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from breaching the SSC User Agreement; and

(4) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from tortiously interfering with Polyakova's Employment Agreement with SSC or with any other SSC employees' contracts with SSC.

19. This action also seeks money damages against SAFE for: misappropriating SSC's trade secrets and confidential and proprietary information, including the Master East List, the CISO Prospect Lists, and the Platform Materials; breaching the User Agreement; tortiously interfering with Polyakova's Employment Agreement with SSC; and engaging in unfair competition.

PARTIES

20. Plaintiff, SSC is a corporation organized under the laws of the State of Delaware with its principal place of business in New York, New York. SSC has offices at 1140 Avenue of the Americas, New York, New York 10036.

21. Defendant SAFE is a corporation organized under the laws of the State of Delaware with its principal place of business, upon information and belief, in Palo Alto, California.

22. Upon information and belief, Defendant Polyakova is a resident of Sunbury, Ohio. Polyakova was employed as a Sales Director at SSC from February 17, 2020 until April 9, 2024. Although Polyakova worked remotely, she reported to a manager based in New York and managed four to five sales representatives, one of whom lived in New York and had a regular physical presence in SSC's New York office.

23. Upon information and belief, Polyakova began working for SAFE as its Vice President, Central Sales, on or about May 30, 2024.

JURISDICTION AND VENUE

24. This Court has subject-matter jurisdiction over this action under 28 U.S.C. § 1331 because the action arises, *inter alia*, under the Defend Trade Secrets Act, 18 U.S.C. § 1836, *et seq.* ("DTSA").

25. The Court has supplemental jurisdiction over the state law claims alleged herein pursuant to 28 U.S.C. § 1367.

26. This Court has personal jurisdiction over Defendants pursuant to CPLR § 302(a)(1)-(3) because Defendants SAFE and Polyakova each transacted business and provided services within the State of New York related to the claims herein, each committed tortious acts within the State of New York that caused injury to SSC in the State of New York, and each

committed tortious acts outside the State of New York causing injury to SSC in the State of New York.

27. Venue is proper in the Southern District of New York pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to this action occurred within this judicial district.

28. Jurisdiction and venue are also proper in this Court because SAFE agreed in the User Agreement that "all disputes arising out of or relating to this Agreement are limited to the exclusive jurisdiction and venue of the state and federal courts located within New York County, New York. Each party hereby consents to and waives any objections with respect to such jurisdiction and venue." *See* Ex. A.

FACTUAL ALLEGATIONS

SSC's Business

29. Formed in 2013, SSC is a privately-held technology company that has pioneered the cybersecurity risk management field. SSC measures and rates the security of digital infrastructure worldwide and helps businesses and governments monitor cybersecurity threats around their cloud-based security. It does so, *inter alia*, by utilizing a complex algorithm that takes billions of impressions of the internet daily to find potential vulnerabilities and security holes, generating a cybersecurity score for an organization's digital assets.

30. SSC's security ratings allow its customers to identify, understand and manage security risks to their own information systems, as well as the information systems of organizations with whom they work or share data (*e.g.,* third parties, such as vendors and suppliers). SSC offers its security ratings platform to organizations globally, including organizations based in the State of New York.

31. SSC's security ratings services are sold by slot, meaning, for example, that an organization seeking to monitor the security vulnerabilities of ten of its third-party supply chain vendors, would purchase ten such monitoring slots. By purchasing these slots, customers are given access to SSC's comprehensive ratings database containing ratings for millions of organizations around the world.

32. SSC also offers complimentary "freemium" access to its security ratings platform, whereby organizations can self-monitor their own ratings score and see high-level security scores of five other organizations without any detailed information (which requires the purchase of slots). *See* https://securityscorecard.com/platform/. In many instances, "freemium" trial customers convert into paying customers once they see the capabilities and benefits of SSC's platform, and its ability to provide insights into other businesses, beyond their own, by purchasing slots and other products and services.

33. SSC also offers its customers a suite of bespoke professional cybersecurity advisory services, including real-time threat monitoring, digital forensic responses, and third-party cyber risk management.

34. SSC sells its professional cybersecurity advisory services to organizations globally, including organizations based in the State of New York.

35. The typical contract value for SSC's security ratings and professional advisory services is in the tens of thousands of dollars per year.

36. With cyberattacks on enterprise networks rapidly rising, and given recent technological advances in artificial intelligence, cybersecurity has become an increasing focus of some of the world's biggest and most profitable companies. Thousands of companies – including the country's biggest banks, pharmaceutical companies, and insurance companies (industries

prone to third-party supply chain security threats) – already rely upon SSC and its cutting-edge platform and advisory services to identify vulnerabilities and prevent online attacks.

37. As cyberterrorism tactics become ever more sophisticated, SSC spends considerable time, energy and resources to stay ahead of the curve, developing innovative counter-techniques and strategies.

38. SSC also spends considerable time, energy and resources identifying prospects and customers. Approximately 85 of SSC's 189 U.S. employees work full-time in its Revenue Organization, which is principally comprised of its Business Development Representatives ("BDR") and its Sales Department. SSC's 28-person BDR Department works solely on identifying prospects and generating customer leads. Once a lead is identified, the account is turned over to one of the approximately 35 SSC Sales Directors, who then further identify customer needs, conduct product demonstrations and close customer deals.

39. Since its inception, SSC has expended over $200 million to develop its customer and prospect base.

40. SSC's customer and prospect list is the direct result of years of marketing and sales efforts, and cannot be replicated through publicly available sources.

41. SSC therefore undertakes considerable efforts to maintain the secrecy of its Confidential Information, including the Master East List and the CISO Prospect Lists. Among other things, SSC's intranet is password protected with multi-factor authentication and role-based permission restrictions. SSC restricts access to information about customers and prospects to those personnel whose access is necessary to their sales, marketing and/or customer servicing activities. Moreover, all personnel provided such access are subject to confidentiality, non-competition and

non-solicitation restrictive covenants, and all employees are required to acknowledge Company policies barring, *inter alia*, emailing confidential documents to their personal email addresses.

42. SSC also provides its employees with Company-issued laptops and mobile phone technology to further protect its Confidential Information.

Polyakova Joins SSC and Is Provided Access to SSC Trade Secrets and Confidential and Proprietary Information

43. On February 8, 2020, Polyakova was hired by SSC as a Sales Director, with a start date of February 17, 2020. On January 4, 2021, Polyakova was given the title of Regional Sales Director. On June 1, 2022, Polyakova was promoted to Director, Sales, Central Region – the title she held until her separation from SSC.

44. In her role as Sales Director, Polyakova conducted product demonstrations and sold access to SSC's security ratings platform and SSC's professional consulting services.

45. Although Polyakova worked remotely, she reported to a manager based in New York and managed at least one sales representative based in New York. Therefore, she remotely interacted with SSC personnel in the State of New York on a daily, or near-daily, basis. She participated in new hire training in New York, and she came to New York on at least one other occasion to attend an SSC meeting. Her SSC email signature, which she used regularly to conduct business and which she used to send to her personal GMail email account the Master East List and CISO Prospect Lists, listed SSC's office address in New York.

46. At SSC, customer and prospect information is stored centrally in SSC's Salesforce database. As a Sales Director, Polyakova had access to that Salesforce database, and to SSC customer work product, customer and prospect proposals, and information about customer current and future needs. She also managed four to five sales representatives who covered SSC customers

with locations in states recorded in the Master East List. Her role with the Company necessitated her access to such information.

47. Polyakova's February 8, 2020 Offer Letter ("Offer Letter") required that, as an express condition of her employment, she would sign the Employment Agreement, and would "keep strictly confidential all trade secrets and information that Company holds proprietary or confidential." *See* Ex. F.

48. Polyakova's Offer Letter further provided that Polyakova would receive an annual base salary, and that she would be eligible to participate in a commission plan pursuant to which she would receive the same amount as her base salary if she achieved 100% of the commission plan.

49. It is not unusual in the cybersecurity industry for sales representatives to receive half their pay through these kinds of bonus incentives. It would therefore not be unusual for half of Polyakova's pay at SAFE to be incentive-based, just as it was at SSC.

50. On February 8, 2020, Polyakova signed her SSC Employment Agreement. *See* Ex. B. Among other things, in that agreement, Polyakova agreed to "keep in confidence and trust all Proprietary Information, and [] not directly or indirectly disclose, sell, use, lecture upon or publish any Proprietary Information or anything relating to it without the prior written consent of the Company." *Id*. § 1(a).

51. "Proprietary Information" is defined in the SSC Employment Agreement as:

> [I]nformation that has been created, discovered or developed, or has otherwise become known to the Company (including without limitation information created, discovered, developed or made known by or to me during the period of or arising out of my employment by the Company), and/or in which property rights have been assigned or otherwise conveyed to the Company, which information has commercial value in the business in which the Company is engaged," including "(a) inventions, confidential knowledge, trade secrets, ideas, data, programs, works of

> authorship, know-how, improvements, discoveries, designs, techniques and sensitive information the Company receives from its customers or receives from a third party under obligation to keep confidential; (b) technical information relating to the Company's existing and future products, including, where appropriate and without limitation, manufacturing techniques and procedures, production controls, software, firmware, information, patent disclosures, patent applications, development or experimental work, formulae, engineering or test data, product specification and part lists, names of suppliers, structures, models, techniques, processes and apparatus relating to the same disclosed by the Company to me or obtained by me through observation or examination of information or developments; (c) **confidential marketing information (including without limitation marketing strategies, customer names and requirements and product and services, prices, margins and costs**); (d) confidential future product plans; (e) confidential financial information provided to me by the Company; (f) personnel information (including without limitation employee compensation); and (g) other confidential business information.

Id., Ex. A § 1.4 (emphasis added).

52. Notably, in the SSC Employment Agreement, Polyakova also expressly "acknowledge[d] and agree[d] that the names, addresses and specifications of the Company's business partners and other associates constitute Proprietary Information and that the sale or unauthorized use or disclosure of this or any other Proprietary Information that [she] obtained during the course of this Agreement would constitute unfair competition with the Company." *See id*. § 4(a).

53. Polyakova's SSC Employment Agreement contains a New York choice-of-law clause (*id.* § 19), and a binding arbitration requirement that carves-out requests for injunctive relief (*id.* § 19, Ex. C).

54. Pursuant to her Offer Letter, upon her hiring, Polyakova was granted options to purchase Company stock, subject to the terms of the Company's Stock Option Agreement.

55. All SSC employees, including Polyakova, are also required to read, accept and follow SSC's Employee Handbook. Polyakova accepted the terms of the Employee Handbook on November 29, 2022.

56. Under a subheading titled "Communication & Computer Systems," the Employee Handbook provides:

> **Employees are prohibited from using personal e-mail accounts or text messaging applications to conduct Company business. Employees may not forward Company emails to a personal email address.** Employees may not use any third party email or instant messaging accounts or services (such as **GMail**, WhatsApp, Yahoo, etc.) for business purposes or any purpose on the Company's computer systems that are not ordinarily used in the performance of their job duties.

Ex. C § IV.C (emphasis added).

57. Under a subheading titled "Confidential Information & Conflicts of Interest," the Employee Handbook provides:

> Employees may learn confidential information, including trade secrets, about the Company. Confidential information are items of information relating to the Company, its services, products, clients/customers, suppliers, vendors, and business partners that are not generally known or available to the general public, but have been developed, compiled or acquired by the Company at its great effort and expense. **Confidential information includes, but is not limited to:** business model, methods, operations, strategies, plans for future business, marketing initiatives, products, services, **customer information and lists, finances, and revenues**. Each employee must safeguard confidential Company information. Confidential information may not be disclosed or distributed to any individual or entity, or used for the benefit of any individual or entity other than the Company, without prior written consent. Employees may not use their position, influence, knowledge of confidential information, including trade secrets, or the Company's assets for personal commercial gain, for the benefit of any competing company or organization, or for the benefit of any other third party except as may be required in performance of their duties as employees of the Company.

Id. § IV.F (emphasis added).

58. All SSC employees, including Polyakova, are also required to read, accept, and follow SSC's Acceptable Use Policy. Ex. D. Polyakova accepted the terms of SSC's Acceptable Use Policy on October 16, 2023.

59. Among other things, the Acceptable Use Policy provides: "You agree not to use personal email accounts for, but not limited to: Dissemination of confidential information." *Id.* at p. 5.

SAFE Surreptitiously Accesses SSC's Platform and Downloads and Exports SSC's Platform Materials

60. SAFE is undeniably a direct SSC competitor in the security ratings space and, in particular, the third-party risk management sector.

61. Upon information and belief, SAFE offers competitive products and services to businesses throughout the United States, including businesses based in the State of New York.

62. In late 2023, SAFE registered for a freemium account to SSC's security ratings platform, which allowed it only to check its own rating and see high-level security scores of five other organizations. Like all freemium account users, SAFE agreed to SSC's User Agreement, which unambiguously provided in the preamble:

> You may not access the Services or request information from our Services if you are a direct competitor of SSC, except with our prior written consent. In addition, you may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other competitive purposes.

Ex. A.

63. SAFE further agreed in the User Agreement that it would never access SSC's platform "in order to build a competitive product or service or use [SSC's cybersecurity ratings and related third-party risk management services] in a way that competes with products or services offered by SSC." Ex. A.

64. The User Agreement also expressly states that SSC services, and any proprietary materials provided through the services, constituted SSC confidential information. *Id*.

65. The User Agreement contains a New York choice-of-law clause and a New York choice of venue clause, providing that "all disputes arising out of or relating to this Agreement are limited to the exclusive jurisdiction and venue of the state and federal courts located within New York County, New York. Each party hereby consents to and waives any objections with respect to such jurisdiction and venue." Ex. A.

66. At the time SAFE registered for a freemium account, SSC understood SAFE would use its access to the platform only to self-monitor its own security score and see limited information about the high-level security scores of five other companies.

67. It has now become clear, however, that SAFE impermissibly accessed the SSC platform for competitive purposes – an intent SAFE itself now admits on its own website, when comparing SSC's product offerings to its own, in an effort to encourage SSC customers and prospects to use SAFE's products and services instead. *See* Ex. G (comparing SAFE's and SSC's product offerings, features, methodologies, and pricing, based on a "review done [in] May 2024").

68. Even more troubling, the Internet Protocol (IP) address of one of the users accessing SSC's platform under SAFE's account ("Anurag.p@safe.security") was an exact match to the IP address of another user of a *paid* account surreptitiously registered to Starlit Group. Anurag Pal, upon information and belief, was employed by SAFE as a Principal Scientist.

69. Further investigation revealed that Starlit Technologies Private Limited had previously purchased 5 slots on SSC's platform. A purchase order listing Starlit Technologies Private Limited as the end-user identifies the "Contact Person" as "Nakul" with the contact email address "infosec@starlitgroup.net." Further investigation revealed that

"anurag.pal@safe.security" and "infosec@starlitgroup.net" repeatedly accessed SSC's platform using the same user agent—a string of characters representing a person (e.g., a browser on the Web) containing descriptions of the operating systems and device type that the user is running—between December 22, 2023 and January 30, 2024.

70. Upon further investigation, it was discovered that at least four separate IP addresses reflected activity on SSC's platform associated with both SAFE and Starlit Group, including repeated use and login to SSC's platform between September 26, 2023 and April 16, 2024.

71. At least three SAFE employees had accounts directly tied to the Starlit Group during their employment with SAFE, and used those accounts to log onto the Platform—Anurag Pal (SAFE's Principal Scientist from October 2022 through April 2024), Nakul Khandelwal (SAFE's Director of Product Management from April 2018 through November 2023), and a SAFE employee with the email address "sb@safe.security" (used to log onto SSC's platform in January 2022).

72. Those individuals accessed and used SSC's platform at a dramatically higher rate than typical SSC customers, and exported more documents and information from SSC's platform than any other SSC customers subscribed to the same plan offering, and did so, upon information and belief, to advance SAFE's competitive standing.

73. The paid account registered under starlitgroup.net has been very active, and until it was recently shut down, was unlawfully pulling significant data from SSC's platform.

74. Accordingly, upon information and belief, SAFE was utilizing Starlit Group as a proxy to surreptitiously and impermissibly access the SSC platform to download and export SSC's work product to enhance and improve SAFE's own competitive product offerings and gain a competitive advantage.

SAFE Arranges Bogus Hiring Interviews with SSC Employees to Learn About SSC's Business Model

75. At least as of April 9, 2024, SAFE had begun regularly "interviewing" SSC employees and former employees under the false guise of potential employment, with the true purpose of gathering intelligence about SSC's business plans and Confidential Information.

76. Incredibly, SAFE openly admitted employing this tactic when, on April 9, 2024, SAFE's Co-Founder and Chief Executive Officer, Saket Modi, bragged to SSC's President, Sachin Bansal, that SAFE was interviewing former SSC employees with no real intention of hiring them for open positions.

77. As proof of these illicit fact-finding endeavors, Mr. Modi touted to Mr. Bansal confidential statistics on SSC's hiring and restructuring practices learned during the employee interviews.

SSC Sends Cease-and-Desist Letters; SAFE Denies Any Wrongdoing

78. On May 3, 2024, counsel for SSC sent SAFE a cease-and-desist letter demanding that SAFE immediately cease its deliberate and unlawful campaign to misappropriate SSC Confidential Information through fake hiring interviews and by tortiously interfering with its former employees' agreements with SSC – notably, the confidentiality and non-competition restrictive covenants contained therein. SSC warned that if SAFE's illicit activities continued, SSC would immediately commence litigation. Ex. H.

79. SAFE responded on May 7, 2024. SAFE admitted it had "interviewed some candidates who were employed with [SSC]" but claimed its interviews were "in the ordinary course of business" and acts of "fair competition," despite oral acknowledgments to the contrary by SAFE's own Co-Founder and CEO. Ex. I.

80. SAFE also denied possessing or utilizing SSC trade secrets, claiming that any information obtained from newly-hired SSC former employees merely came from their "general experience in the industry." *Id*. SAFE did not deny that it had seen SSC employment agreements – containing the very same confidential and non-competition restrictions contained in Polyakova's Employment Agreement.

81. After learning that Andrew Peck ("Peck"), another SSC employee, had accepted, or was intending to accept, a position with SAFE, on May 14, 2024, SSC counsel sent a separate cease-and-desist letter to Peck, demanding that he, too, comply with his agreement with SSC. Ex. J.

82. Throughout Peck's multi-year employment with SSC, he was a resident of the State of New York. Upon information and belief, Peck currently still resides in the State of New York.

83. On May 21, 2024, counsel for SAFE responded to the May 14 letter to Peck, denying, *inter alia*, any attempt by SAFE to misappropriate SSC Confidential Information. Ex. K.

Polyakova, After Stealing SSC's Master East List and CISO Prospect Lists, Joins SAFE as Vice President, Central Sales

84. On or about May 21, 2024, SSC discovered that, on January 4, 2024, Polyakova, while still working at SSC, impermissibly sent the Master East List via email to her personal GMail email account, in blatant disregard of her SSC Employment Agreement, Offer Letter, Employee Handbook and Acceptable Use Policy.

85. The Master East List is a compilation of 9,262 records, comprised of over 500 customers, or approximately one-fifth of SSC's entire customer base as of January 4, 2024, and thousands of SSC prospects. The Master East List contains over 1,000 customers and prospects based in the State of New York.

86. Thereafter, on March 27 and 28, 2024, Polyakova also sent the CISO Prospect Lists to her personal GMail email account – two files collectively containing detailed contact information for over 200 CISO-level prospects, and the individual contacts at each such prospect, compiled by SSC as a way to track invites and RSVPs to two business development events.

87. Polyakova's employment with SSC was terminated on April 9, 2024.

88. Upon information and belief, Polyakova's first day of work at SAFE was on or around May 30, 2024.

89. Upon information and belief, Polyakova, with SAFE's knowledge and assistance, intends to use the Master East List and the CISO Prospect Lists stolen from SSC to encourage SSC customers to leave SSC and bring their business to SAFE – including over one thousand customers and prospects based in the State of New York.

90. As confirmation of SAFE's intent to capitalize on the Master East List and CISO Prospect Lists to capture SSC customers, one need look no further than a May 7, 2024 blog post created by SAFE, explicitly offering "50% OFF current security rating contracts, subscription transfers from SecurityScorecard." Ex. L.

91. Upon information and belief, SSC customers have left SSC for SAFE, and prospective SSC customers have gone with SAFE instead of SSC.

92. In a May 30, 2024 LinkedIn post announcing her new position with SAFE, Polyakova stated she is seeking to hire sales representatives in six of the states specifically covered in the Master East List. *See* Ex. E.

93. SAFE has unlawfully accessed the SSC platform under disguise, to gain an unfair competitive advantage over SSC; Polyakova, while employed by SSC, stole the Master East List

and CISO Prospect Lists; SSC customers have departed for SAFE; and Polyakova joined SAFE as its Vice President, Central Sales, armed with the Master East List and the CISO Prospect Lists.

94. SSC now seeks injunctive relief to prevent the otherwise inevitable and irreparable harm it faces.

FIRST CAUSE OF ACTION
Permanent Injunctive Relief
(against SAFE and Polyakova)

95. SSC repeats and realleges paragraphs 1-94 as if fully set forth herein.

96. As alleged above, Polyakova intentionally and wrongfully sent to her personal GMail email account SSC trade secrets and confidential and proprietary information, including SSC's Master East List containing detailed confidential and proprietary information regarding 9,262 SSC customers and prospects, and the CISO Prospect Lists, containing detailed confidential and proprietary information about over 200 CISO-level prospects.

97. If SAFE were to obtain the Master East List and/or CISO Prospect Lists, it would risk the potential destruction of a substantial portion of SSC's core business.

98. Upon information and belief, Polyakova is now SAFE's Vice President, Central Sales, and has already shared and/or used for SAFE's benefit, SSC's trade secrets and confidential and proprietary information, including the Master East List and CISO Prospect Lists, threatening SSC with irreparable injury.

99. SAFE has also unlawfully accessed and exported documents and information from SSC's platform, under disguise, to gain an unfair competitive advantage over SSC.

100. SSC has no adequate remedy at law for SAFE's and Polyakova's misconduct. SSC cannot be fully compensated for its injuries by a damages award if Defendants are permitted to

continue to improperly use, maintain, or transmit SSC Confidential Information, including the Master East List and the CISO Prospect Lists and information obtained from SSC's platform.

101. Once information of this type is known by a direct competitor, there is no way to un-ring that bell through monetary damages alone; injunctive relief is indispensable.

102. Moreover, Polyakova likely lacks the resources to compensate SSC for the harm she has caused, is causing, and/or will cause, absent such injunctive relief.

103. Defendants' intentional and wrongful conduct, as described above, unless and until permanently enjoined and restrained by Order of this Court, will disrupt the status quo and cause irreparable injury to SSC.

104. Accordingly, SSC seeks permanent injunctive relief as follows:

(1) enjoining Polyakova, SAFE, and all persons acting in concert with or through them who receive actual notice of the injunction, from using or disclosing the Master East List, the CISO Prospect Lists, the Platform Materials, or any other SSC trade secrets or confidential or proprietary information;

(2) enjoining Polyakova from further breaching the confidentiality obligations contained in her Employment Agreement with SSC;

(3) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from breaching the SSC User Agreement; and

(4) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from tortiously interfering with Polyakova's Employment Agreement with SSC or with any other SSC employees' contracts with SSC.

SECOND CAUSE OF ACTION

Violation of The Defend Trade Secrets Act, 18 U.S.C. 1836, et seq.
(against SAFE and, for injunctive relief only, against Polyakova)

105. SSC repeats and realleges paragraphs 1-104 as if fully set forth herein.

106. SSC trade secrets include the Master East List and the CISO Prospect Lists.

107. These trade secrets give SSC a significant advantage over its competitors — an advantage that would be lost if such trade secrets became known to SSC's competitors, such as SAFE.

108. These trade secrets derive independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from their disclosure or use.

109. SSC has made reasonable efforts to protect the confidentiality of these trade secrets, including protecting its intranet with multi-factor authentication and role-based permission restrictions; restricting access to only those employees whose responsibilities necessitated access; requiring all Company employees who had access to sign employment agreements containing confidentiality, non-competition and non-solicitation restrictive covenants; requiring all employees to acknowledge Company policies barring, *inter alia*, emailing confidential documents to their personal email addresses; and providing Company-issued computers and mobile phone technology to employees to ensure that SSC confidential information remained on SSC devices and networks.

110. Polyakova had knowledge of, and access to, SSC's trade secrets and confidential and proprietary information, including the Master East List and CISO Prospect Lists.

111. Polyakova was and remains under a duty to keep SSC's trade secrets and confidential and proprietary information confidential, and not to use, exploit or divulge such information, other than for the benefit of SSC and with its authorization.

112. Polyakova misappropriated SSC's trade secrets for her own personal gain and, upon information and belief, SAFE's gain, without regard to SSC's rights, and without compensation, permission, or license from SSC.

113. Upon information and belief, SAFE intends to utilize such information to solicit SSC's customers and prospects in its East Region to purchase SAFE's products and services used in interstate commerce.

114. Upon information and belief, SAFE's and Polyakova's conduct was and remains willful and wanton, in bad faith and with blatant disregard for SSC's valid and enforceable rights. As a result, SSC is also entitled to punitive, exemplary damages against SAFE under 18 U.S.C. § 1836(b)(3)(C), in an amount not more than two times the amount of SSC's actual losses and unjust enrichment damages, and reasonable attorneys' fees under 18 U.S.C. § 1836(b)(3)(D).

115. As a result of SAFE's and Polyakova's conduct, SSC has been, and is still being, damaged in an amount to be determined at trial.

116. SSC has suffered and will suffer irreparable harm as a result of Defendants' conduct — harm that cannot be adequately redressed at law, unless the Court enters injunctive relief:

(1) enjoining Polyakova, SAFE, and all persons acting in concert with or through them who receive actual notice of the injunction, from using or disclosing the Master East List, the CISO Prospect Lists, or any other SSC trade secrets or confidential or proprietary information;

(2) enjoining Polyakova from further breaching the confidentiality obligations contained in her Employment Agreement with SSC;

(3) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from breaching the SSC User Agreement; and

(4) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from tortiously interfering with Polyakova's Employment Agreement with SSC or with any other SSC employees' contracts with SSC.

THIRD CAUSE OF ACTION

Misappropriation of Trade Secrets and Confidential and Proprietary Information (against SAFE and, for injunctive relief only, against Polyakova)

117. SSC repeats and realleges paragraphs 1-116 as if fully set forth herein.

118. SSC possesses the trade secrets and confidential and proprietary information detailed herein, including the Master East List, the CISO Prospect Lists, and the Platform Materials.

119. Those trade secrets and that confidential and proprietary information give SSC a significant advantage over its competitors — an advantage that would be lost if such trade secrets and confidential and proprietary information became known to SSC's competitors, such as SAFE.

120. If the Master East List, CISO Prospect Lists, and the Platform Materials were in the hands of a competitor, it would potentially threaten the destruction of a substantial portion of SSC's business.

121. The trade secrets and confidential and proprietary information derive independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from their disclosure or use.

122. SSC has made reasonable efforts to protect the confidentiality of the trade secrets and confidential and proprietary information, including protecting access to its intranet via multi-factor authentication and role-based permission restrictions; restricting access to only those employees whose responsibilities necessitated access; requiring all Company employees who had access to sign employment agreements containing confidentiality, non-competition and non-

solicitation restrictive covenants; requiring all employees to acknowledge Company policies barring, *inter alia*, emailing confidential documents to their personal email addresses; and providing Company-issued computers and mobile phone technology to employees to ensure that SSC confidential information remained on SSC devices and networks.

123. In addition to the efforts illustrated above, SSC took additional efforts to protect the confidentiality of the Platform Materials, including ensuring such materials are only available to SSC customers after they register for unique user accounts which are password protected and have optional multi-factor authentication protection, and only after such customers have agreed to an End User SaaS Agreement forbidding access by or for direct competitors of SSC and prohibiting use of the Platform Materials for "any competitive purposes."

124. Polyakova had knowledge of, and access to, SSC's trade secrets and confidential and proprietary information, including the Master East List and CISO Prospect Lists.

125. Polyakova was and remains under a duty to keep SSC's trade secrets and confidential and proprietary information confidential and not to use, exploit or divulge such information, other than for the benefit of SSC and with its authorization.

126. Polyakova misappropriated SSC's trade secrets and confidential and proprietary information for her own personal gain and, upon information and belief, SAFE's gain, without regard to SSC's rights, and without compensation, permission, or license from SSC.

127. Upon information and belief, SAFE intends to utilize such information to solicit SSC's customers and prospects in its East Region to purchase SAFE's products and services used in interstate commerce.

128. SAFE, through a paid account registered to a proxy based in India, gained access to, downloaded, and exported SSC's trade secrets and confidential and proprietary information, including the Platform Materials.

129. SAFE, as a direct competitor of SSC, was forbidden from accessing the trade secrets and confidential and proprietary information and was prohibited from using the trade secrets and confidential and proprietary information for "any competitive purposes."

130. Upon information and belief, SAFE misappropriated the impermissibly accessed trade secrets and confidential and propriety information for competitive purposes to enhance and improve SAFE's own competitive product offerings for the purpose of securing a competitive advantage.

131. Upon information and belief, SAFE's and Polyakova's conduct was and remains willful and wanton, in bad faith and with blatant disregard for SSC's valid and enforceable rights. As a result, SSC is also entitled to punitive damages against SAFE.

132. As a result of SAFE's and Polyakova's conduct, SSC has been, and is still being, damaged in an amount to be determined at trial.

133. SSC has suffered irreparable harm as a result of Defendants' conduct and will suffer irreparable harm that cannot be adequately redressed at law, unless and until the Court enters injunctive relief:

(1) enjoining Polyakova, SAFE, and all persons acting in concert with or through them who receive actual notice of the injunction, from using or disclosing the Master East List, the CISO Prospect Lists, the Platform Materials, or any other SSC trade secrets or confidential or proprietary information;

(2) enjoining Polyakova from further breaching the confidentiality obligations contained in her Employment Agreement with SSC;

(3) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from breaching the SSC User Agreement; and

(4) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from tortiously interfering with Polyakova's Employment Agreement with SSC or with any other SSC employees' contracts with SSC.

FOURTH CAUSE OF ACTION
Breach of Contract – SSC User Agreement
(against SAFE)

134. SSC repeats and realleges paragraphs 1-133 as if fully set forth herein.

135. SAFE entered into the SSC User Agreement, pursuant to which SAFE was provided highly limited access to SSC's security ratings platform and databases.

136. The User Agreement is a valid and fully enforceable agreement.

137. SAFE has breached the User Agreement by accessing SSC's platform through a paid account registered to a proxy based in India, and downloading and exporting SSC's work product, to enhance and improve SAFE's own competitive product offerings or use the platform in a way that competes with products or services offered by SSC.

138. SSC performed all conditions, covenants, and promises required by the terms and conditions of the SSC User Agreement.

139. SSC has been damaged, and is still being damaged, by SAFE's contract breaches, in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
Tortious Interference with Contract
(against SAFE)

140. SSC repeats and realleges paragraphs 1-139 as if fully set forth herein.

141. Polyakova's Employment Agreement with SSC is a valid and enforceable contract.

142. Upon information and belief, SAFE had full knowledge of the existence of the Employment Agreement between SSC and Polyakova, including her confidentiality restrictions therein.

143. Despite knowledge of those contractual obligations, SAFE tortiously interfered with them by, upon information and belief, encouraging and facilitating the misappropriation of SSC trade secrets and confidential and proprietary information and/or by using SSC trade secrets and confidential and proprietary information to compete with SSC.

144. SAFE's acts were intentional and conducted with the purpose of interfering with Polyakova's Employment Agreement with SSC.

145. As a direct result of SAFE's tortious interference, SSC has been, and is still being, damaged in an amount to be determined at trial.

146. SAFE has acted in an egregious, malicious, willful and wanton manner, and in bad faith when committing the acts alleged above. As a result, SSC is also entitled to punitive damages against SAFE.

147. SSC has suffered irreparable harm as a result of SAFE's conduct and will continue to suffer irreparable harm that cannot be adequately redressed at law, unless SAFE is enjoined from engaging in any such further tortious interference.

SIXTH CAUSE OF ACTION
Unfair Competition Under New York Common Law
(against SAFE)

148. SSC repeats and realleges paragraphs 1-147 as if fully set forth herein.

149. SAFE's acts constitute unfair competition in violation of the common law of the State of New York.

150. SSC invested considerable time, energy and resources to create its Confidential Information, including but not limited to the Master East List and CISO Prospect Lists.

151. In fact, SSC has spent over $40 million in business development efforts required to assemble these particular lists.

152. Upon information and belief, SAFE has intentionally misappropriated the Master East List, the CISO Prospect Lists and other SSC Confidential Information, with the bad faith intent to take advantage of SSC's reputation, goodwill, and efforts and expenditures, and as such, SAFE has committed unfair competition.

153. Upon information and belief, SAFE has misappropriated the Master East List, the CISO Prospect Lists and other SSC Confidential Information, for its own commercial advantage over SSC by, *inter alia*, attempting to divert and/or actually diverting business away from SSC.

154. SAFE has also engaged in unfair competition by impermissibly accessing SSC's security ratings customer platform to surreptitiously quality check, and reshape, SAFE's own customer offerings, in clear violation of contractual and legal prohibitions on SAFE doing so. By misappropriating the results of the skill, expenditures and labor of SSC in creating its security ratings platform, SAFE has acted in bad faith, exploiting a commercial advantage that belonged exclusively to SSC.

155. The calculated effort by SAFE to undermine SSC has put SSC unfairly at a competitive disadvantage.

156. The foregoing acts of SAFE have injured and will continue to injure SSC, by depriving it of sales of its services, and by injuring its business reputation, all in violation of the common law of the State of New York.

157. SAFE's acts have caused irreparable harm and SSC is entitled to injunctive relief barring SAFE from any further use of the Master East List, CISO Prospect Lists and any other SSC Confidential Information. SSC otherwise has no adequate remedy at law.

158. SSC has been, and is still being, damaged by SAFE's unfair competition, in an amount to be determined at trial.

159. Upon information and belief, SAFE's conduct was and remains willful and wanton, malicious, in bad faith and with blatant disregard for SSC's valid and enforceable rights. As a result, SSC is also entitled to punitive damages against SAFE.

PRAYER FOR RELIEF

WHEREFORE, SSC respectfully requests that the Court enter judgment in favor of SSC and against Defendants, awarding SSC:

(a) Injunctive relief:

(1) enjoining Polyakova, SAFE, and all persons acting in concert with or through them who receive actual notice of the injunction, from using or disclosing the Master East List, the CISO Prospect Lists, the Platform Materials, or any other SSC trade secrets or confidential or proprietary information;

(2) enjoining Polyakova from further breaching the confidentiality obligations contained in her Employment Agreement with SSC;

(3) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from breaching the SSC User Agreement; and

(4) enjoining SAFE, and all persons acting in concert with or through SAFE who receive actual notice of the injunction, from tortiously interfering with Polyakova's Employment Agreement with SSC or with any other SSC employees' contracts with SSC.

(b) Compensatory damages against SAFE in an amount to be determined at trial;

(c) Punitive damages against SAFE in an amount to be determined at trial;

(d) Attorneys' fees and costs;

(e) Pre- and post-judgment interest; and

(f) Such other and further relief as the Court deems just and proper.

Respectfully submitted,

Dated: January 31, 2025

CARLTON FIELDS, P.A.

By: */s/ Michael D. Margulies*

Michael D. Margulies
Michael T. Hensley
405 Lexington Ave., 36th Floor
New York, NY 10174-3699
Tel: (212) 430-5500
Fax: (212) 430-5501
mmargulies@carltonfields.com
mhensley@carltonfields.com

Attorneys for Plaintiff, SecurityScorecard, Inc.